

D-Link DVA-G3672B

Introduction

We have already tested several wireless ADSL routers, DSLAM D-Link [DAS-3248EC](#) included, but today the guest in our laboratory is not just another simple modem, but a device that has a wide array of voice functions. Let's sort through its capabilities in more detail.



External design

ADSL2+ D-Link DVA-G3672B wireless router comes in a black plastic case with rounded corners and a grey stripe on the sides. The device has dimensions of 218x148x35 mm (not considering the antenna). To work properly DVA-G3672B needs an external power unit with the following characteristics: 12V and 5A.



D-Link DVA-G3672B

Written by Administrator

Wednesday, 20 February 2013 14:03 -



On the upper panel of the device there is a brand tag and ventilation grate.



Side panels of DVA-G3672B are not remarkable at all.



Now let's have a look at the insides of the case.

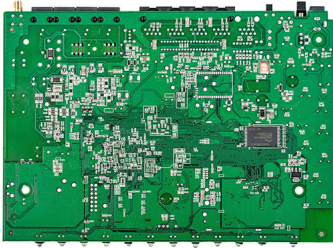
Hardware

The electronic stuffing of DVA-G3672B is one green textolite card which has all essential elements located on one of its sides. The only exception is [Spansion S29GL064N90TFI04](#) flash memory module with the size of 8 Mbytes.

D-Link DVA-G3672B

Written by Administrator

Wednesday, 20 February 2013 14:03 -



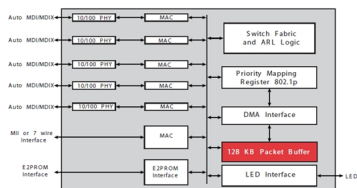
[Broadcom](#) BCM4318KFBG chip and [SiGe](#) [2521A60](#) amplifier act as the wireless module. A chart for Fast Ethernet Broadcom BCM5325EKQMG switch with five ports used is presented below. We have already seen such kind of a switch previously in ASUS

[WMVN25E2+](#)

and ASUS

[DSL-G31](#)

devices.



Voice processing means are carried out by [Legerity](#) (Zarlink/Microsemi) [Le88221DLC](#) module, while

[Broadcom](#)

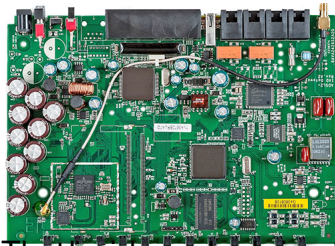
[BCM6358KFBG](#)

performs functions of a SoC with support of ADSL2+. Also, it would be fair to note

[Samsung](#)

[K4H561638H](#)

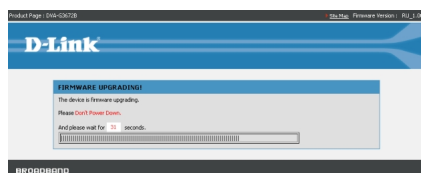
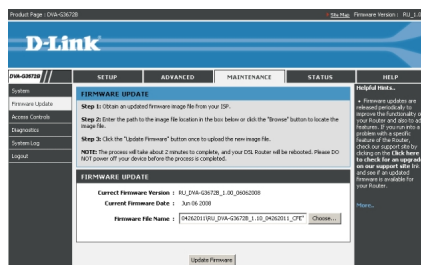
RAM module with the size of 32 Mbytes.



Conclusion: we have passed on the review of capabilities of platform software D-Link DVA-G3672B to a

Firmware update

Firmware update is carried out in Firmware Update menu item, MAINTENANCE tab of the web-interface.



The whole firmware update process takes about two minutes and does not require any technical proficiency from an administrator. It is easy enough, one just needs to choose a file with the new firmware version and click on Update Firmware button.

The same can be performed by using the device command line (/Management/Update Software/Update Software). However, it's worth noticing that in this case one would need to have a TFTP server.

Update Software Menu

1. Update Software

2. Exit

/ Management/Update Software -> 1

Update Software

Press <enter> to use current value

Press <esc> and <enter> to cancel

Tftp Server IP address (): 192.168.1.3

Update Software File Name (bcm963xx_fs_kernel): RU_DVA-G3672B_1.10_04262011_CFE

app: tftp -g -t i -f RU_DVA-G3672B_1.10_04262011_CFE 192.168.1.3

I call diapkillAllApps

app: ps > /var/pslist

kill process [pid: 608] [name: httpd]...

app: kill -9 608

kill process [pid: 565] [name: snmp]...

app: kill -9 565

kill process [pid: 563] [name: klogd]...

app: kill -9 563

kill process [pid: 559] [name: syslogd]...

app: kill -9 559

kill process [pid: 503] [name: dhcpd]...

app: kill -9 503

kill process [pid: 384] [name: igmp]...

app: kill -9 384

app: iptables -F

app: iptables -t filter -F

app: iptables -t nat -F

app: iptables -t mangle -F

app: rmmod ipt_state

app: rmmod ipt_mark

app: rmmod ipt_limit

app: rmmod ipt_TCPMSS

app: rmmod ipt_REDIRECT

app: rmmod ipt_MASQUERADE

app: rmmod ipt_MARK

app: rmmod ipt_string

app: rmmod ipt_LOG

app: rmmod ipt_FTOS

app: rmmod ip_nat_tftp

app: rmmod ip_nat_irc

app: rmmod ip_nat_ftp

app: rmmod ip_nat_h323

app: rmmod ip_nat_pptp

app: rmmod ip_nat_gre

app: rmmod ip_nat_rtsp

app: rmmod ip_nat_ipsec

app: rmmod ip_conntrack_tftp

app: rmmod ip_conntrack_irc

```
app: rmmod ip_conntrack_ftp
app: rmmod ip_conntrack_h323
app: rmmod ip_conntrack_pptp
app: rmmod ip_conntrack_gre
app: rmmod ip_conntrack_rtsp
app: rmmod ip_conntrack_ipsec
app: rmmod iptable_mangle
app: rmmod ip_conntrack
app: rmmod ip_tables
Remaining modules:
ip_queue 10592 0 - Live 0xc0139000
ipt_mac 672 0 - Live 0xc0133000
ipt_ftos 448 0 - Live 0xc012f000
ipt_FRAGMARK 736 0 - Live 0xc0127000
ipt_u32 66528 0 - Live 0xc0115000
ipt_REJECT 4544 0 - Live 0xc0112000
iptable_raw 544 0 - Live 0xc010c000
ipt_vlanid 448 0 - Live 0xc010a000
ipt_iprange 640 0 - Live 0xc0108000
ipt_vlanprio 448 0 - Live 0xc0106000
ipt_VMARK 736 0 - Live 0xc0102000
ipt_time 1600 0 - Live 0xc00fe000
ipt_connperiod 512 0 - Live 0xc00f9000
ipt_DSCP 960 0 - Live 0xc00f5000
ipt_NOTRACK 672 0 - Live 0xc00de000
ip_conntrack_clear_udp 1280 0 - Live 0xc00dc000
iptable_nat 15632 1 ip_queue, Live 0xc0060000
ip_conntrack 30144 5 ip_queue,ipt_connperiod,ipt_NOTRACK,ip_conntrack_clear_udp,
iptable_nat, Live 0xc008e000
iptable_filter 928 0 - Live 0xc0053000
ip_tables 14144 17 ip_queue,ipt_mac,ipt_ftos,ipt_FRAGMARK,ipt_u32,ipt_REJECT,ipt
able_raw,ipt_vlanid,ipt_iprange,ipt_vlanprio,ipt_VMARK,ipt_time,ipt_connperiod,i
pt_DSCP,ipt_NOTRACK,iptable_nat,iptable_filter, Live 0xc0024000
gpio 1824 2 - Live 0xc0013000
endpointdd 1289584 0 - Live 0xc029b000
dspdd 609696 1 endpointdd, Live 0x8104ca80
wl 928896 0 - Live 0xc01b7000
bcm_enet 25376 0 - Live 0xc004b000
bcmprocfs 17200 0 - Live 0xc0018000
br2684 67360 0 - Live 0xc0039000
blaa_dd 7104 0 - Live 0xc0015000
adslidd 142816 0 - Live 0xc006a000
atmapi 56768 3 br2684,blaa_dd,adslidd, Live 0xc002a000
Memory info:
Number of processes: 45
12:03am up 4 min,
```

D-Link DVA-G3672B

Written by Administrator

Wednesday, 20 February 2013 14:03 -

load average: 1 min:0.01, 5 min:0.07, 15 min:0.03

	total	used	free	shared	buffers
Mem:	29412	26304	3108	0	2700
Swap:	0	0	0		
Total:	29412	26304	3108		

Done removing processes

Allocating 4405444 bytes for broadcom image.

Memory allocated

Total image size: 4405465

Broadcom format verified.

Tftp image done. call after parselImageData

Flashing CFE...

```
#####  
##### The device is firmware upgrading... #####  
##### Please Do not Power Down..... #####  
#####
```

After that the router will automatically reboot itself and get ready for further work.

Another firmware update method is using a built-in TFTP server. One only needs to upload the firmware update file to it. An example of the command that uploads the necessary file to the TFTP server in Windows OS is presented below.

```
tftp -i 192.168.1.1 put c:RU_DVA-G3672B_1.10_04262011_CFE
```

Now let's review capabilities of D-Link DVA-G3672B web-interface.

Web-interface

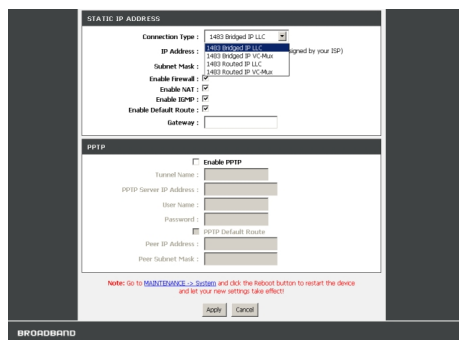
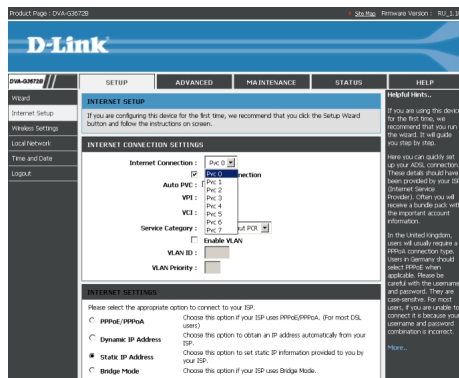
In order to access the device web-interface one should use any modern browser and type in logon information upon authorisation; it is admin/admin by default.



The web-interface design is common for all devices by this brand. We would like to inform our

readers beforehand that we will not review all capabilities of DVA-G3672B, but only turn our attention to the most interesting features.

By using Internet Setup menu item an administrator can manage up to eight simultaneous connections to the provider used to transfer data, receive IPTV services, or for any other purposes.



We would like to give a bit of explanation on the available connection types. The following data encapsulation process will take place upon choosing a connection type starting with Bridged IP: IP->Ethernet->ATM. While upon choosing Routed IP the data encapsulation process will be as follows: IP->ATM. If it's necessary, the administrator can also create a PPTP tunnel over the connection that has been already created.

Wireless Basics and Wireless Security sections in Wireless Settings menu item of SETUP tab

Written by Administrator
Wednesday, 20 February 2013 14:03 -

ADMIN	DESIGN	ADVANCED	MAINTENANCE	STATUS	HELP
WIRELESS SECURITY					
<div> <div> <p>Use the section to configure the wireless settings for your Cisco Router. Please note that changes will also need to be duplicated to your wireless clients and PCs.</p> <p>Wireless Basics</p> <p>Wireless Settings</p> <p>Wireless Security</p> <p>Wireless Status</p> <p>Wireless Logs</p> </div> <div> <p>To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WPA, WPA2, and WPA3.</p> <p>The WPA2 mode is the original wireless encryption standard. WPA2 provides a higher level of security.</p> <p>For maximum compatibility, use WPA. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode. The best security, use WPA2 mode. This mode uses AES/CCMP cipher and legacy devices are not allowed access to your network. WPA3 (or WPA2) mode to achieve a balance of strong security and broad compatibility. WPA3 is required for Secure Connect, but is not required for legacy devices with performance that are WPA2 capable. Also the strongest cipher that the client supports will be used.</p> <p>To achieve better wireless performance use WPA2 security mode (or in other words AES cipher).</p> </div> </div>					
<div> <div> <p>Wireless Network Name (SSID) <input type="text" value="Cisco-Diva-036702"/></p> <p>Security Mode: <input type="text" value="WPA2"/> (AES)</p> </div> <div> <p>WPA2</p> <p>WPA Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.</p> <p>WPA Mode: <input type="text" value="WPA2 (AES)"/> (AES)</p> <p>Group Key Update Interval: <input type="text" value="60 seconds"/> (seconds)</p> </div> </div>					
<p>Please take note of your SSID as you will need to configure the same settings to your wireless devices and PCs.</p>					
<div> <div> <p>Apply</p> <p>Cancel</p> </div> <div> <p>Helpful Links</p> <p>If you have wireless devices, security may be required. If you enter down the page, you will see the configuration. If you need to change the configuration, you need to change the configuration on any wireless device that you connect to your wireless network.</p> <p>View...</p> </div> </div>					

9 / 20

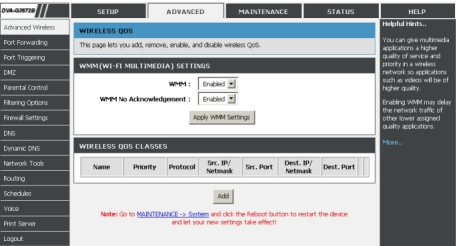
Managing the data synchronisation parameters with servers over the Internet is performed using Time and Date menu item. Unfortunately, the device time zones do not include the day-light saving time amendments which were recently made in the Russian legislature.

The screenshot shows the 'TIME AND DATE' configuration page in the D-Link DVA-G3672B web interface. The page is divided into three main sections: 'TIME AND DATE', 'NTP SETTINGS', and 'TIME CONFIGURATION'. The 'TIME AND DATE' section contains a description of the Time Configuration option and a 'Helpful Hints...' link. The 'NTP SETTINGS' section includes a checkbox for 'Automatically synchronize with Internet time servers' and two dropdown menus for 'First NTP Time Server' (set to 'ntp1.dlink.com') and 'Second NTP Time Server' (set to 'none'). The 'TIME CONFIGURATION' section shows the 'Current Router Time' as 'Sun 01, 2008 00:25:18', a 'Time Zone' dropdown set to '(GMT+03:00) Moscow, St. Petersburg, Volgograd', and a checkbox for 'Enable Daylight Saving' which is currently unchecked. Below this, there are fields for 'Daylight Saving Offset' and 'Daylight Saving Dates' with 'Start' and 'End' date pickers. A note at the bottom states: 'Note: Go to MAINTENANCE > Setup and click the Reboot button to restart the device and let your new settings take effect.' There are 'Apply' and 'Cancel' buttons at the bottom right.

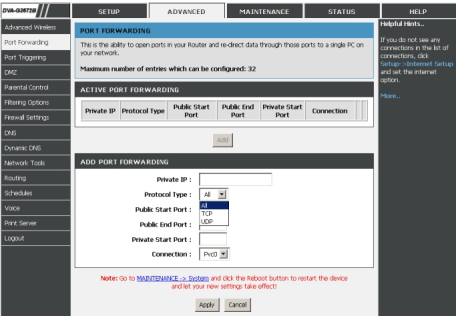
In order to carry out a more detailed adjustment of the wireless network segment one needs to use sections of Advanced Wireless menu item, ADVANCED tab. Over here the administrator can manage filtering of the wireless clients through MAC-addresses and change QoS parameters.

The screenshot shows the 'ADVANCED WIRELESS' configuration page in the D-Link DVA-G3672B web interface. The page is divided into two main sections: 'ADVANCED WIRELESS' and 'ADVANCED WIRELESS SETTINGS'. The 'ADVANCED WIRELESS' section contains a description of the settings and a 'Helpful Hints...' link. The 'ADVANCED WIRELESS SETTINGS' section includes several configuration options: 'Transmission Rate' (set to 'Auto'), 'Multicast Rate' (set to 'Auto'), 'Transmit Power' (set to '100%'), 'Beacon Period' (set to '100' with a range of '20 ~ 65535'), 'RTS Threshold' (set to '2347' with a range of '0 ~ 2347'), 'Fragmentation Threshold' (set to '2346' with a range of '256 ~ 2346'), 'DTIM Interval' (set to '1' with a range of '1 ~ 255'), and 'User Isolation' (set to 'Off'). There is also a checkbox for 'Enable Wireless Guest Network' which is currently unchecked. A note at the bottom states: 'Note: It is strongly recommended that you configure wireless security for Guest SSID once you enable it.' There are 'Apply' and 'Cancel' buttons at the bottom right.

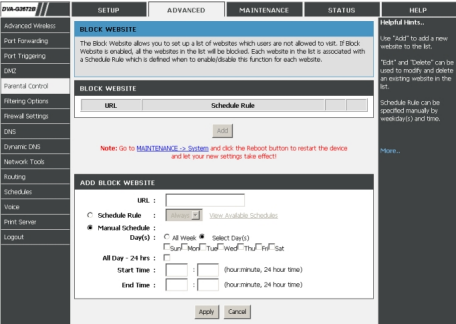
The screenshot shows the 'WIRELESS MAC FILTERING' configuration page in the D-Link DVA-G3672B web interface. The page is divided into two main sections: 'WIRELESS MAC FILTERING' and 'WIRELESS MAC FILTERING LIST'. The 'WIRELESS MAC FILTERING' section contains a description of the settings and a 'Helpful Hints...' link. The 'WIRELESS MAC FILTERING LIST' section includes a table with a header 'MAC Address' and a single row with an empty cell. Below the table is an 'Add' button. A note at the bottom states: 'Note: Go to MAINTENANCE > Setup and click the Reboot button to restart the device and let your new settings take effect.' There are 'Apply' and 'Cancel' buttons at the bottom right.



Port Forwarding, Port Triggering, and DMZ menu items are used to provide access to the internal services from the WAN.



By using sections in Parental Control menu item one can filter the access to certain WAN resources from various nodes according to schedule.



D-Link DVA-G3672B

Written by Administrator

Wednesday, 20 February 2013 14:03 -

Advanced Wireless

Port Forwarding

Port Triggering

DMZ

Parental Control

Filtering Options

Internal Settings

DNS

Dynamic DNS

Network Tools

Routing

Schedules

VoIP

Port Server

Logout

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

BLOCK MAC ADDRESS

The Block MAC Address allows you to set up a list of MAC addresses of LAN devices which will be restricted to access the Internet. If the Block MAC address option is enabled, all the LAN devices with the MAC address in the list will not be allowed to access the Internet. Each MAC address in the list is associated with a Schedule Rule which is defined when to enable/disable the function for each MAC address.

Block MAC ADDRESS

Username	MAC Address	Schedule
<div>ADD</div>		

ADD BLOCK MAC ADDRESS

Username :

Current PC's MAC Address : 00:0C:8C:00:00:00 (device connected)

Other MAC Address : (device connected)

Schedule Rule :

Manual Schedule

Day(s) :

all

Select Day(s)

Start Time :

00:00

 (hour:minute, 24 hour time)

End Time :

00:00

 (hour:minute, 24 hour time)

Helpful Hints...

Use "Add" to add a new MAC address to the list.

"Start" and "End" can be used to modify and delete an existing MAC address in the list.

Schedule Rule can be specified manually by weekDay(s) and time.

More...

INCOMING IP FILTERING

The Inbound Filter allows you to create filter rules to allow the incoming traffic from Internet based on IP range and protocol. Each filter rule is specified by a filter name and at least one condition.

By default, all incoming IP traffic from the Internet is blocked when the firewall is enabled, but some IP traffic can be ACCEPTED by setting up filters.

INBOUND FILTERING

Filter Name	Protocol	Source Address	Source Port	Dest. Address	Dest. Port
<div>ADD</div>					

ADD INBOUND IP FILTERING

Filter Name :

Protocol :

all

 (Click to Select)

Select IP Range by :

IP address

255.255.255.255

 (Start or port/port)

Source IP Address :

255.255.255.255

 (Network)

Select IP Range by :

Network

255.255.255.255

 (port or port/port)

Destination IP Address :

255.255.255.255

 (port or port/port)

Destination Subnet Mask :

255.255.255.255

 (port or port/port)

Helpful Hints...

If you want the IP address, port, and network mask to be "any", just leave them empty.

The Port value can be fixed with a single port or a range of ports. (Separating port ending ports).

More...

BRIDGE FILTERING

Bridge Filtering is only effective on a PC configured in Bridge mode. ALLOW means that all MAC layer frames will be ALLOWED except those matching with any of the specified rules in the following table. DENY means that all MAC layer frames will be DENIED except those matching with any of the specified rules in the following table.

The Active Bridge Filter allows you to Create a filter which is specified by the MAC layer frames and at least one condition. If multiple conditions are specified, all of them will take effect.

Bridge Filtering Global Policy:

ALLOW all packets but DENY those matching any of specific rules listed

DENY all packets but ALLOW those matching any of specific rules listed

ACTIVE BRIDGE FILTERS

Protocol	Distribution MAC	Source MAC	Frame Direction
<div>ADD</div>			

ADD BRIDGE FILTER

Protocol Type :

PPPOE

Destination MAC Address :

00:00:00:00:00:00

Source MAC Address :

00:00:00:00:00:00

Frame Direction :

Both

Helpful Hints...

Note: You must first create a Bridge connection to use Bridge Filter.

You can create a Bridge connection by going to Setup -> Advanced Setup.

More...

FIREWALL SETTINGS

The Router already provides a simple firewall by virtue of the way NAT works. By default NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet observations.

FIREWALL SETTINGS

Enable SPI

Enable DOS and Portscan Protection

SYN/ACK reset attack

SYN/ACK attack

SYN/FIN attack

Ping (Ping of Death) attack

Flood (Flood) attack

Null scanning attack

Helpful Hints...

More...

QOS

You can set the Quality of Service on the web page. This should improve performance of Internet applications like games, video, voice, etc.

IP QOS

Please set configuration for IP-based QoS.

PVC :

Enable Upstream Rate Limit

Bandwidth :

64

 (Kbps)

Enable Classification Control

Classification :

TOS

Port Mapping

Port	Weight	Range (0-7)
UDP	<div>100</div> %	<div>0</div> - <div>10</div>
ACSL	<div>100</div> %	<div>0</div> - <div>10</div>
SRAP	<div>100</div> %	<div>0</div> - <div>10</div>
TR-069	<div>100</div> %	<div>0</div> - <div>10</div>

Helpful Hints...

If you want to enable the QoS function, please enable Port Mapping first. QoS is only used with dynamic mode PVC. Bridge mode PVC is not supported now.

QOS

You can set the Quality of Service on the web page. This should improve performance of Internet applications like games, video, voice, etc.

IP QOS

Please set configuration for IP-based QoS.

PVC :

Enable Upstream Rate Limit

Bandwidth :

64

 (Kbps)

Enable Classification Control

Classification :

TOS

Port Mapping

Port	Weight	Range (0-7)
UDP	<div>100</div> %	<div>0</div> - <div>10</div>
ACSL	<div>100</div> %	<div>0</div> - <div>10</div>
SRAP	<div>100</div> %	<div>0</div> - <div>10</div>
TR-069	<div>100</div> %	<div>0</div> - <div>10</div>

Helpful Hints...

If you want to enable the QoS function, please enable Port Mapping first. QoS is only used with dynamic mode PVC. Bridge mode PVC is not supported now.

D-Link DVA-G3672B can be configured to get traffic for filtering. Options are a router and

One can switch to protection against DOS attacks in Firewall Settings menu items.

One can switch to QoS in Port Mapping menu items. One can also set the router to be a bridge mode and

12 / 20

Written by Administrator
Wednesday, 20 February 2013 14:03 -

are responsible for routing. Apart from static routing,

manage the connection of two analogue phones of

Written by Administrator
Wednesday, 20 February 2013 14:03 -



The **System** menu item in the **MAINTENANCE** tab allows rebooting the device and performing standard

porters of control. the administrator can specify the access

Printer Discovery tool connects the local network segment and access to the Internet resources

Brief information about the device is located in Device Info menu item, STATUS tab.

Stateful table distribution of STAP LAG devices using DHCP receive information table also was checked.

D-Link DVA-G3672B

Written by Administrator
Wednesday, 20 February 2013 14:03 -

The first screenshot shows the 'TRAFFIC STATISTICS' tab. It includes a 'LOCAL NETWORK & WIRELESS' section with a table for Ethernet and Wireless traffic, and an 'INTERNET' section with a table for VPL/VEI traffic. Below these are ADSL statistics including Mode, Type, Line Coding, Status, and various error counts.

The second screenshot shows the 'ROUTING TABLE' tab. It includes a 'ROUTING TABLE LISTS' section with a table showing Destination, Gateway, Genmask, Flags, Metric, Ref, Use, and Interface.

The third screenshot shows the 'HELP' tab. It includes a 'HELP MENU' section with links to Setup, Advanced, Maintenance, and Status. Below this are 'SETUP HELP' and 'ADVANCED HELP' sections with detailed links to various configuration options.

Help information on each section and menu item of the web-interface is available in HELP tab.

Examining the capabilities of the mainline web-interface to a conclusion and pass on to

Command line interface

Access to the command line can be granted or prohibited using Access Control menu item, MAINTENANCE tab. One must use the same logon information as for the connection to the device web-interface. Upon successful authentication an administrator will find him/herself in the menu. It's worth noticing that the command line interface design as a menu appeared in firmwares beginning from 1.10 version.

Note: If you have problem with Backspace key, please make sure you configure your terminal emulator settings.

For instance, from HyperTerminal you would need to use File->Properties->Setting->Back Space key sends.

Main Menu

1. ADSL Link State
2. LAN
3. WAN
4. DNS Server
5. Route Setup
6. NAT

7. Firewall
8. Quality Of Service
9. Management
10. Passwords
11. Diag
12. Reset to Default
13. Save and Reboot
14. Exit

Information on the ADSL operation is located in the first item.

-> 1

ADSL Link Info

adsl: ADSL driver and PHY status

Status: IdleRetrain Reason: 0

Link Power State: L0

Hit <enter> to continue

The second and third items contain configuration of LAN and WAN interfaces, correspondingly.

LAN Menu

1. Configure
2. Show
3. Exit

/ LAN -> 2

Show LAN Menu

IP Address 192.168.1.1

Netmask 255.255.255.0

Ethernet Speed Auto

Ethernet Type Auto

Ethernet MTU 1500

DHCP Server Disabled

Hit <enter> to continue

WAN Menu

1. Configure
2. Show
3. Exit

/ WAN -> 2

PVC	VCC	Con.	Catego.	Service	Interface	Proto.	IGMP	QoS	State	Status
-----	-----	------	---------	---------	-----------	--------	------	-----	-------	--------

ID	Name	Name	address
1	0.8.35 1	UBR pppoe_0_8_35_1	ppp_0_8_35_1 PPPoE Enable Disable
5	0.0.41 1	UBR br_0_41	nas_0_0_41 Bridge N/A Disable Disable Disable
2	0.0.42 1	UBR br_0_42	nas_0_0_42 Bridge N/A Disable Disable Disable
3	0.0.43 1	UBR br_0_43	nas_0_0_43 Bridge N/A Disable Disable Disable

Enable ADSL Link Down

```

4    0.0.44 1    UBR    br_0_44    nas_0_0_44    Bridge N/A    Disable Disable Disable
6    0.0.45 1    UBR    br_0_45    nas_0_0_45    Bridge N/A    Disable Disable Disable
7    0.0.46 1    UBR    br_0_46    nas_0_0_46    Bridge N/A    Disable Disable Disable
8    0.0.47 1    UBR    br_0_47    nas_0_0_47    Bridge N/A    Disable Disable Disable
Hit <enter> to continue

```

Access to the routing settings can be gained using the fifth item.

Route Setup Menu

1. Default Gateway
2. Add Route
3. Delete Route
4. Show Route
5. RIP
6. Exit

/ Route Setup -> 4

Routing Table Show Menu

Flags: U - up, ! - reject, G - gateway, H - host, R - Reinststate
 D - dynamic (redirect), M - modified (redirect)

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	*	255.255.255.0	U	0	0	0	br0

Hit <enter> to continue

The password management is performed in item 10.

Password Menu

1. Admin
2. User
3. Support
4. Exit

/Passwords -> 1

Password Configuration Menu For User admin

Note: Maximum length of password is 16 characters.

Old password :

New password :

Confirm new password:

app: echo 0 > /var/isdft_cfg

Password for admin changed successfully.

Hit <enter> to continue

The user can carry out the line diagnostics in item 11.

Diagnostics Menu

1. OAM Diagnostics Menu
2. Exit

/Diag ->1

OAM Diagnostics Menu

1. Test ATM OAM Loopback

2. Exit

/Diag/OAM Diagnostics Menu ->1

Press <enter> to use current value

Press <esc> and <enter> to cancel

ManagementType [f4, f5] (f5):

Type [segment, end] (end):

Press <enter> to use current value

Press <esc> and <enter> to cancel

port [0-3] (0):

vpi [0-256] (0):

vci [32-65535] (33):

ATM F5 OAM Loopback (End) Test: FAIL

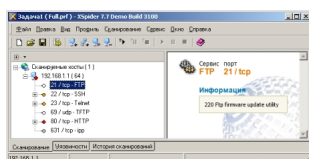
Hit <enter> to continue

That's where we proceed to completion of the brief review of command line capabilities of the device switch and pass on to testing it.

Testing

The first testing procedure we usually begin our testing section with is estimating the booting time of the device, which is a time interval starting with the moment when the power is on until the first echo reply is received through ICMP protocol. D-Link DVA-G3672B boots in 31 seconds. We believe that the result is decent.

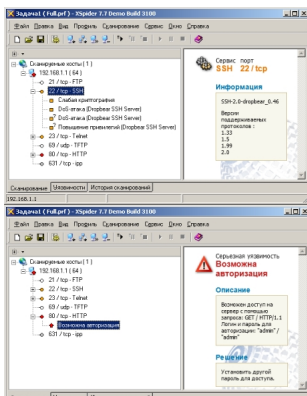
The next thing we usually do is conducting a security scanning procedure, which has been carried out using Positive Technologies XSpider 7.7 (Demo build 3100) utility. On the whole, there were six open ports discovered, and they are TCP-21 (FTP), TCP-22 (SSH), TCP-23 (Telnet), UDP-69 (TFTP), TCP-80 (HTTP) and TCP-631 (ipp). The most interesting data detected are presented below.



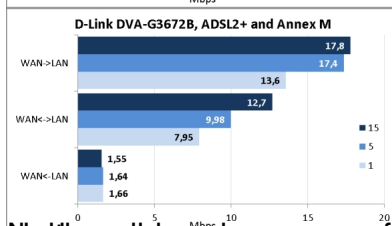
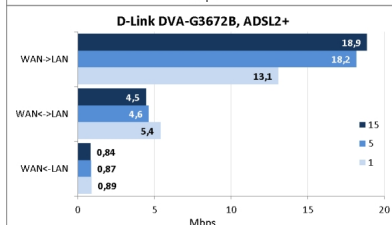
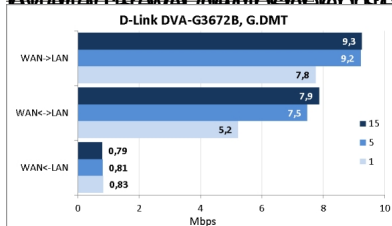
D-Link DVA-G3672B

Written by Administrator

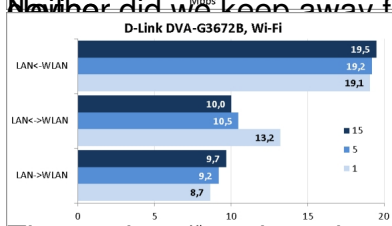
Wednesday, 20 February 2013 14:03 -



As the state of things is not ideal, we do not limit ourselves to the data transfer speed through ADSL not limiting ourselves



Number did we keep away from performance tests of the wireless network segment of the



That's where we draw the testing chapter to a close and move on to summing it all up.

Conclusion

Judging by the functional capabilities of D-Link DVA-G3672B wireless router it'd be fair to notice that this device is intended for use in small offices or workshops. VoIP support will probably be useful for both enterprise and home users.

Among the strength areas of device are the following.

D-Link DVA-G3672B

Written by Administrator

Wednesday, 20 February 2013 14:03 -

- Support of SIP
- Competitive price
- Support of dynamic routing and SNMP
- Ability to turn off the wireless network using a hardware switch
- Support of Annex M
- Presence of a print server

Unfortunately, we cannot help to mention several drawbacks of this model.

- A TFTP server in LAN network is available to everyone by default
- Incorrect time zones for Russia
- Both analogue phones can work only with one SIP service

As of when this article was being written, the average price for a D-Link DVA-G3672B in Moscow online shops was 2200 roubles.